

Practical 2

Aim: User Administration

1. Manage local users, groups and creation of multiple users from excel sheet
2. Control access to files

Commands for reference:

System Administrator: su, adduser, addgroup, rmuser, shutdown

Control Access: chmod, umask

PART A

Manage local users, groups and creation of multiple users from excel sheet

| | |
|---------|---|
| Que. | <ol style="list-style-type: none"> 1. Run id command to view the current user and group information. 2. display the current working directory. 3. print the value of HOME and PATH variable to determine the home directory and user's executable's path respectively. 4. Run su and su - command. Observe the output for the same.what is the main difference between them? 5. Run sudo su at the shell prompt to become the root user. 9. Exit the current user's shell to return to the student user's shell |
| Command | <ol style="list-style-type: none"> 1. id 2. pwd 3. echo \$HOME 4. echo \$PATH 5. su 6. su - <ul style="list-style-type: none"> • su: Switches to the target user's shell but retains the current environment. • su -: Switches to the target user's shell and initiates a new login shell, effectively switching to the target user's environment. 7. sudo su 8. exit |

| | |
|----------|--|
| Output | <pre> ubuntu@ubuntu:~\$ id uid=1000(ubuntu) gid=1000(ubuntu) groups=1000(ubuntu),4(adm),24(cdrom),27(sudo), 30(dip),46(plugdev),100(users),114(lpadmin),124(sambashare) ubuntu@ubuntu:~\$ pwd /home/ubuntu ubuntu@ubuntu:~\$ echo \$HOME /home/ubuntu ubuntu@ubuntu:~\$ echo \$PATH /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:/snap/bin ubuntu@ubuntu:~\$ su Password: ubuntu@ubuntu:~\$ sudo su root@ubuntu:/home/ubuntu# ^C root@ubuntu:/home/ubuntu# ^C root@ubuntu:/home/ubuntu# exit exit ubuntu@ubuntu:~\$ </pre> |
| Que | <p>10. Attempt to view the last five lines of /var/log/auth.log without using sudo</p> <p>11. Attempt to view the last five lines of /var/log/auth.log using sudo</p> <p>12. Attempt to make a copy of /etc/rpc as /etc/rpcOLD without using sudo</p> <p>13. Attempt to make a copy of /etc/rpc as /etc/rpcOLD with sudo.</p> <p>14. Attempt to delete /etc/rpcOLD without using sudo</p> <p>15. Attempt to delete /etc/rpcdOLD with sudo</p> |
| Commands | <p>10.tail -n 5 /var/log/auth.log</p> <p>11.sudo tail -n 5 /var/log/auth.log</p> <p>12.cp /etc/rpc /etc/rpcOLD</p> <p>13.sudo cp /etc/rpc /etc/rpcOLD</p> <p>14.rm /etc/rpcOLD</p> <p>15.sudo rm /etc/rpcOLD</p> |

| | |
|----------|---|
| Output | <pre> ubuntu@ubuntu:~\$ tail -n 5 /var/log/auth.log 2024-07-18T10:43:27.945081+00:00 ubuntu su[11327]: pam_unix(su:session): session opened for user root(uid=0) by ubuntu(uid=0) 2024-07-18T10:43:41.972474+00:00 ubuntu su[11327]: pam_unix(su:session): session closed for user root 2024-07-18T10:43:41.975250+00:00 ubuntu sudo: pam_unix(sudo:session): session closed for user root 2024-07-18T10:45:01.665624+00:00 ubuntu CRON[11343]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0) 2024-07-18T10:45:01.673330+00:00 ubuntu CRON[11343]: pam_unix(cron:session): session closed for user root ubuntu@ubuntu:~\$ sudo tail -n 5 /var/log/auth.log 2024-07-18T10:43:41.975250+00:00 ubuntu sudo: pam_unix(sudo:session): session closed for user root 2024-07-18T10:45:01.665624+00:00 ubuntu CRON[11343]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0) 2024-07-18T10:45:01.673330+00:00 ubuntu CRON[11343]: pam_unix(cron:session): session closed for user root 2024-07-18T10:45:38.040559+00:00 ubuntu sudo: ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/tail -n 5 /var/log/auth.log 2024-07-18T10:45:38.050451+00:00 ubuntu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu(uid=1000) ubuntu@ubuntu:~\$ cp /etc/rpc/etc/rpcOLD cp: missing destination file operand after '/etc/rpc/etc/rpcOLD' Try 'cp --help' for more information. ubuntu@ubuntu:~\$ cp /etc/rpc/etc/rpcOLD </pre> |
| Que | <p>16. check the UID for root user, administrator and local users.</p> <p>17. Adduser user01.</p> |
| Commands | <p>10. id -u root</p> <p>getent group sudo</p> <p>id root</p> <p>11. sudo adduser user01</p> |
| Output | <pre> ubuntu@ubuntu:~\$ id -u root 0 ubuntu@ubuntu:~\$ getent group sudo sudo:x:27:ubuntu,installer ubuntu@ubuntu:~\$ id root uid=0(root) gid=0(root) groups=0(root) ubuntu@ubuntu:~\$ sudo adduser user01 info: Adding user `user01' ... info: Selecting UID/GID from range 1000 to 59999 ... info: Adding new group `user01' (1002) ... info: Adding new user `user01' (1002) with group `user01 (1002)' ... info: Creating home directory `/home/user01' ... info: Copying files from `/etc/skel' ... New password: BAD PASSWORD: The password is shorter than 8 characters Return your password: </pre> |

```

tematic
Retype new password:
passwd: password updated successfully
Changing the user information for user01
Enter the new value, or press ENTER for the default
    Full Name []: user01
    Room Number []: 1
    Work Phone []: 9988776655
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
info: Adding new user `user01' to supplemental / extra groups `user
info: Adding user `user01' to group `users' ...
ubuntu@ubuntu:~$

```

| | |
|----------------|---|
| Que. | <p>18. Create the group group01 with the GID of 10000.</p> <p>19. Create the group group02</p> <p>20. Examine /etc/group to verify the supplemental group memberships.</p> |
| Command | <p>18. sudo addgroup --gid 10000 group01</p> <p>19. sudo addgroup group02</p> <p>20. cat /etc/group</p> |
| Output | <pre> ubuntu@ubuntu:~\$ sudo groupadd -g 1001 grp2 groupadd: GID '1001' already exists ubuntu@ubuntu:~\$ sudo groupadd -g 2001 grp2 ubuntu@ubuntu:~\$ sudo group add grp3 sudo: group: command not found ubuntu@ubuntu:~\$ sudo groupadd grp3 ubuntu@ubuntu:~\$ cat /etc/group root:x:0: daemon:x:1: bin:x:2: sys:x:3: adm:x:4:syslog,ubuntu,installer tty:x:5: disk:x:6: lp:x:7: mail:x:8: news:x:9: uucp:x:10: man:x:12: proxy:x:13: kmem:x:15: dialout:x:20:installer fax:x:21: voice:x:22: </pre> |

| | |
|----------------|--|
| Que. | |
| Command | |
| Output | <pre> fwupd-refresh:x:989: scanner:x:115:saned saned:x:116: geoclue:x:117: pipewire:x:118: polkitd:x:988: rtkit:x:119: colord:x:120: gdm:x:121: nm-openvpn:x:122: lxd:x:123:installer ubuntu:x:1000: smbshare:x:124:ubuntu gamemode:x:987: gnome-initial-setup:x:986: gnome-remote-desktop:x:985: installer:x:1001: user01:x:1002: group01sudo:x:10000: group02:x:10001: grp1:x:10002: grp2:x:2001: grp3:x:10003: ubuntu@ubuntu:~\$ </pre> |

| | |
|----------------|---|
| Que. | 21. Use the usermod -aG command to add a user to a supplementary group. Add user01 to the group created. 22. Observe /etc/group and /etc/passwd |
| Command | 21. sudo usermod -aG group01 user01 22. cat /etc/group |

Output

```
ubuntu@ubuntu:~$ sudo usermod -aG grp31 user01
usermod: group 'grp31' does not exist
ubuntu@ubuntu:~$ sudo usermod -aG grp3 user01
ubuntu@ubuntu:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,ubuntu,installer
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:installer
fax:x:21:
voice:x:22:

fwupd-refresh:x:989:
scanner:x:115:saned
saned:x:116:
geoclue:x:117:
pipewire:x:118:
polkitd:x:988:
rtkit:x:119:
colord:x:120:
gdm:x:121:
nm-openvpn:x:122:
lxd:x:123:installer
ubuntu:x:1000:
sambashare:x:124:ubuntu
gamemode:x:987:
gnome-initial-setup:x:986:
gnome-remote-desktop:x:985:
installer:x:1001:
user01:x:1002:
group01sudo:x:10000:
group02:x:10001:
grp1:x:10002:
grp2:x:2001:
grp3:x:10003:user01
ubuntu@ubuntu:~$
```

PART B

Control access to files

| | |
|----------------|--|
| Que. | 1. Check the permission of files created. 2. Check the permission of directories created. 3. Set read and write permissions for others with numeric mode to file1.txt 4. Remove write permission for user, group and others to folder CE. |
| Command | 1. ls -l file2.txt 2. ls -ld CE 3. chmod 666 file1.txt 4. chmod a-w CE |
| Output | <pre> ubuntu@ubuntu:~\$ ls -l total 0 drwxrwxr-x 3 ubuntu ubuntu 60 Jun 27 18:29 CSPIT drwxr-xr-x 2 ubuntu ubuntu 60 Jun 27 15:43 Desktop drwxr-xr-x 2 ubuntu ubuntu 40 Jun 27 15:44 Documents drwxr-xr-x 2 ubuntu ubuntu 40 Jun 27 15:44 Downloads drwxr-xr-x 2 ubuntu ubuntu 40 Jun 27 15:44 Music drwxr-xr-x 2 ubuntu ubuntu 40 Jun 27 15:44 Pictures drwxr-xr-x 2 ubuntu ubuntu 40 Jun 27 15:44 Public drwxr-xr-x 2 ubuntu ubuntu 40 Jun 27 15:44 Templates drwxr-xr-x 2 ubuntu ubuntu 40 Jun 27 15:44 Videos drwx----- 5 ubuntu ubuntu 100 Jun 27 18:00 snap ubuntu@ubuntu:~\$ ubuntu@ubuntu:~/CSPIT\$ ls -l CE total 36 -rw-rw-r-- 1 ubuntu ubuntu 0 Jun 27 18:29 ce1.txt -rw-rw-r-- 1 ubuntu ubuntu 0 Jun 27 18:30 f3.txt -rw-rw-r-- 1 ubuntu ubuntu 43 Jun 27 18:31 file1.txt -rw-rw-r-- 1 ubuntu ubuntu 38 Jun 27 18:50 file1_no_digits.txt -rw-rw-r-- 1 ubuntu ubuntu 55 Jun 27 18:32 file2.txt -rw-rw-r-- 1 ubuntu ubuntu 56 Jun 27 18:37 file4.txt -rw-rw-r-- 1 ubuntu ubuntu 48 Jun 27 18:39 file5.txt -rw-rw-r-- 1 ubuntu ubuntu 54 Jun 27 18:47 file6.txt -rw-rw-r-- 1 ubuntu ubuntu 60 Jun 27 18:47 file7.txt -rw-rw-r-- 1 ubuntu ubuntu 118 Jun 27 18:52 file8.txt -rw-rw-r-- 1 ubuntu ubuntu 215 Jul 11 15:57 file9.txt ubuntu@ubuntu:~/CSPIT\$ ubuntu@ubuntu:~/CSPIT\$ cd CE ubuntu@ubuntu:~/CSPIT/CE\$ chmod 66 file1.txt] chmod: cannot access 'file1.txt]': No such file or directory ubuntu@ubuntu:~/CSPIT/CE\$ chmod 66 file1.txt ubuntu@ubuntu:~/CSPIT/CE\$ cd ~ ubuntu@ubuntu:~\$ chmod a-w CE chmod: cannot access 'CE': No such file or directory ubuntu@ubuntu:~\$ cd CSPIT ubuntu@ubuntu:~/CSPIT\$ chmod a-w CE ubuntu@ubuntu:~/CSPIT\$ </pre> |

| | |
|-------------|--|
| Que. | 5. Create a directory 5CE under CE. Observe the response. 6. Set read, write and execute permissions for user, group and others to 5CE. 7. Set read and execute permission for group and no permission for other to file2.txt. 8. Change the ownership of file to user01 9. Change the group ownership of file to group01 10. Change the ownership of both group and user at the same time. |
|-------------|--|

| | |
|----------------|--|
| Command | 5. mkdir CE/5CE 6. chmod 777 CE/5CE 7. chmod 750 file2.txt 8. sudo chown user01 file2.txt 9. sudo chown :group01 file2.txt 10. sudo chown user01:group01 file_name |
| Output | <pre> ubuntu@ubuntu:~/CSPIT\$ sudo mkdir 5CE ubuntu@ubuntu:~/CSPIT\$ cd CE ubuntu@ubuntu:~/CSPIT/CE\$ chmod 750 file2.txt ubuntu@ubuntu:~/CSPIT/CE\$ sudo chown user01 file2.txt ubuntu@ubuntu:~/CSPIT/CE\$ ls -l file2.txt -rwxr-x--- 1 user01 ubuntu 55 Jun 27 18:32 file2.txt ubuntu@ubuntu:~/CSPIT/CE\$ sudo chown :grp1 file2.txt ubuntu@ubuntu:~/CSPIT/CE\$ ls -l file2.txt -rwxr-x--- 1 user01 grp1 55 Jun 27 18:32 file2.txt ubuntu@ubuntu:~/CSPIT/CE\$ sudo chown user01:grp1 file2.txt ubuntu@ubuntu:~/CSPIT/CE\$ la -l file2.txt -rwxr-x--- 1 user01 grp1 55 Jun 27 18:32 file2.txt ubuntu@ubuntu:~/CSPIT/CE\$ </pre> |

| | |
|----------------|--|
| Que. | 11. Set the special permissions on directory. a. The <i>setuid</i> permission on an executable file means that commands run as the user owning the file, not as the user that ran the command. One example is the passwd command: run <code>ls -l /usr/bin/passwd</code> b. The special permission <i>setgid</i> on a directory means that files created in the directory inherit their group ownership from the directory, rather than inheriting it from the creating user. run <code>ls -ld /run/log/journal</code> c. the <i>sticky bit</i> for a directory sets a special restriction on deletion of files. Only the owner of the file (and root) can delete files within the directory. run <code>ls -ld /tmp</code> 12. Set the setuid, setgid and sticky bit for different files and perform the operations accordingly. |
| Command | 11. a) <code>ls -l /usr/bin/passwd</code> b) <code>ls -ld /run/log/journal</code> c) <code>ls -ld /tmp</code> 12. <code>sudo chmod u+s file_name</code> <code>sudo chmod g+s directory_name</code> <code>sudo chmod +t directory_name</code> |

Output

```
ubuntu@ubuntu: ~/CSPIT/CE
ubuntu@ubuntu:~/CSPIT/CE$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 64152 Apr  9 12:31 /usr/bin/passwd
ubuntu@ubuntu:~/CSPIT/CE$ ls -ld /run/log/journal
drwxr-sr-x+ 2 root systemd-journal 40 Jun 27 15:43 /run/log/j
ubuntu@ubuntu:~/CSPIT/CE$ ls -ld /tmp
drwxrwxrwt 23 root root 500 Aug  8 12:48 /tmp
ubuntu@ubuntu:~/CSPIT/CE$ sudo chmod u+s file2.txt
ubuntu@ubuntu:~/CSPIT/CE$ ls -l file2.txt
-rwsr-x--- 1 user01 grp1 55 Jun 27 18:32 file2.txt
ubuntu@ubuntu:~/CSPIT/CE$ sudo chmod g+s student
chmod: cannot access 'student': No such file or directory
ubuntu@ubuntu:~/CSPIT/CE$ sudo chmod g+s CE
chmod: cannot access 'CE': No such file or directory
ubuntu@ubuntu:~/CSPIT/CE$ sudo chmod g+s 5CE
ubuntu@ubuntu:~/CSPIT/CE$ ls -ld 5CE
drwxr-sr-x 2 root root 40 Aug  8 13:08 5CE
ubuntu@ubuntu:~/CSPIT/CE$ sudo chmod +t 5CE
ubuntu@ubuntu:~/CSPIT/CE$ ls -ld 5CE
drwxr-sr-t 2 root root 40 Aug  8 13:08 5CE
ubuntu@ubuntu:~/CSPIT/CE$
```

Que.

13. Display the current value of shell's mask.
14. Check the permission of directories.
15. Check the permission of files.
16. Set the umask to 542.
17. Check the permission of files and directories.
18. Try to open the file and directory created.
19. Try to open the file as other user.

Command

13. umask
14. ls -ld directory_name
15. ls -l file_name
16. umask 542
17. touch new_file
mkdir new_directory
ls -l new_file
ls -ld new_directory
18. cat new_file
cd new_directory
19. su another_user
cat new_file

Output

```
ubuntu@ubuntu:~/CSPIT/CE$ sudo mkdir newdir
ubuntu@ubuntu:~/CSPIT/CE$ ls -l ce1.txt
-rw-rw-r-- 1 ubuntu ubuntu 0 Aug  8 13:20 ce1.txt
ubuntu@ubuntu:~/CSPIT/CE$ ls -ld mkdir
ls: cannot access 'mkdir': No such file or directory
ubuntu@ubuntu:~/CSPIT/CE$ ls -ld newdir

drwxr-xr-x 2 root root 40 Aug  8 13:20 newdir
ubuntu@ubuntu:~/CSPIT/CE$ cat ce1.txt
ubuntu@ubuntu:~/CSPIT/CE$ cd newdir
ubuntu@ubuntu:~/CSPIT/CE/newdir$ su another_user
su: user another_user does not exist or the user entry does not contain
the required fields
ubuntu@ubuntu:~/CSPIT/CE/newdir$ adduser another_user
fatal: Only root may add a user or group to the system.
ubuntu@ubuntu:~/CSPIT/CE/newdir$ su user01
Password:
user01@ubuntu:/home/ubuntu/CSPIT/CE/newdir$ cat ce1.txt
```

```
ubuntu@ubuntu:~/CSPIT/CE$ cd newdir
ubuntu@ubuntu:~/CSPIT/CE/newdir$ su user01
Password:
user01@ubuntu:/home/ubuntu/CSPIT/CE/newdir$ cat ce1.txt
user01@ubuntu:/home/ubuntu/CSPIT/CE/newdir$ cat ce1.txt
hello students . hello students
user01@ubuntu:/home/ubuntu/CSPIT/CE/newdir$
```